REMARKS

In accordance with the foregoing, the specification has been amended to improve form and to clarify the statement at page 12, lines 15-17 so as to be consistent with the disclosure at page 5, lines 1-7, page 12, lines 10-17 and the paragraph spanning pages 19-20. In addition, new claims 27-30 have been added, based on claims 1, 9, 19 and 22, but of differing scope and/or style. Claim 3 is amended to correct the dependency thereof and claims 17 and 25 are amended to recite a specific set of "predetermined conversion processes" thereby to more clearly delineate the invention and distinguish same from Kanevsky et al. Further, a new Abstract is presented. No new matter has been presented and, accordingly, approval and entry of the specification and claim amendments, new claims and Abstract are respectfully requested.

In addition, a Letter to the Examiner is filed concurrently, requesting approval of a change in Fig. 9 of the drawings.

ITEM 2: REJECTION OF CLAIMS 1-4, 8-13 AND 17-26 UNDER 35 USC 102(e) AS BEING ANTICIPATED BY USP 6,092,192 OF KANEVSKY

Claims 1-4, 8-13 and 17-26 stand rejected under 35 USC 102(e) as being anticipated by Kanevsky et al. Since the Examiner also rejects claims 5-7 and 14-16 on page 3 of the Office Action, applicants assume that the Examiner intended to reject all of the claims 1-26 on the above grounds.

The rejections are respectfully traversed.

An important feature of the present invention is a "conversion" of original biometric information, relating to an individual and which is to be used for verification purposes, whereby the invention renders it possible to positively prevent the original biometric information from being stolen by a third party, greatly improving security even in a circumstance in which data management reliability is not sufficiently high.

In accordance with a first embodiment of the invention and as shown in Fig. 1A, measured biometric information is first converted and then feature information is extracted from the converted biometric information and the extracted feature information then is compared with registered such information for verification purposes. Claims 1-8 and 19-21 relate to this

embodiment of the invention.

A second embodiment of the invention is shown in Fig. 1B, for example, and which extracts feature information from measured biometric information and converts the extracted feature information and then compares the converted extracted feature information with registered such information for verification purposes. Claims 9-16 and 22-24 are directed to this second embodiment.

The third embodiment of the invention, as shown in Fig. 10, for example, measures biometric (or feature) information, converts the measured biometric (or feature) information and registers the converted biometric (or feature) information. The registered, converted biometric (or feature) information then may be used for authentication in accordance with the further processing of either the first embodiment or the second embodiment. Claims 17 and 25 are directed to this third embodiment; claims 18 and 36 respectively correspond to original claims 17 and 25 but, additionally, recite verifying means.

New claims 27-30 are based on claims 1, 9, 19 and 22, respectively, and while of differing scope, are submitted to be in accordance with the above characterizations of those respective original pending claims.

In contrast to the above-discussed embodiments of the invention, Kanevsky et al. merely proposes an apparatus for providing repetitive enrollment in a plurality of biometric recognition systems based on an initial enrollment. The apparatus includes an extractor for extracting a biometric attribute from a user and a server which is operatively coupled to the extractor. The server interfaces with the plurality of biometric recognition systems to receive requests for biometric attributes therefrom and to transmit encrypted biometric attributes thereto. The server has a memory for storing the encrypted biometric attributes.

Each biometric attribute is encrypted so as to improve security when transmitted from the server to the client. Hence, when a biometric attribute is to be used by a client, the client must decrypt the encrypted biometric attribute using a public key, as explained in col. 5, lines 10-11 of Kanevsky et al.

Kanevsky et al. does not provide a detailed explanation of the verification process employed therein, since the main object of Kanevsky et al. is to facilitate enrollment of a user. However, when using the biometric attribute which is encrypted and stored in the memory of the server, it is clear from col. 5, lines 10-11 that Kanevsky et al. restores the original biometric

attribute, or information, in the client by decrypting the encrypted biometric information. Otherwise, the input biometric attribute (extracted by the extractor) cannot be verified in the client by making a comparison with the decrypted biometric attribute.

Thus, in Kanevsky, the need to decrypt the encrypted biometric attribute in the client makes it possible for a person to steal the original biometric attribute, once it has been decrypted.

On the other hand, according to the first and second embodiments of the present invention, the verification process uses the extracted features of the converted biometric information or the converted information of the extracted features. In other words, the present invention performs the comparison using the information in the converted form, and not in the original form. For this reason, the present invention can positively prevent the original biometric information from being stolen. Even if the information in the converted form, as is used for verification in accordance with the invention, is stolen, this converted information is not of much use to the thief, since it is extremely difficult to derive or restore the original biometric information from this converted information. (See, e.g., specification at page 12, lines 10-17)

As noted above, claims 17 and 25 and claims 18 and 26 relate to the third embodiment of the invention. Claims 17 and 25 have been amended to clarify the "predetermined conversion process" recited in the originally filed claims. As will be appreciated, the specified "conversion" processes of the amended claims 17 and 25 do not include encryption, as is performed in Kanevsky, and which is non-equivalent to the specified conversion processes of the claimed invention.

Claims 18 and 26 readily distinguish over Kanevsky et al. by virtue of the recitation of the verification process in each.

In accordance with the foregoing, it is submitted that the pending claims patentably distinguish over Kanevsky et al.

ITEMS 4-6:

These items all relate to dependent claims which depend from respective ones of the above independent claims and which have been shown to distinguish patentably over the reference--with the sole exception of independent claim 19, included in item 6 and which is addressed hereinabove as patentably distinguishing over Kanevsky et al.

The dependent claims incorporate or inherit the limitations of their respective independent claims and hence share the common patentable distinctions thereof over the reference, in addition to setting forth features establishing new patentable combinations which further patentably distinguish over Kanevsky et al.

CONCLUSION

Accordingly, it is submitted that the pending claims 1-30 distinguish patentably over the art of record. There being no other objections or rejections, it is submitted that the application is in condition for allowance, which action is earnestly solicited.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: January 13, 2003

By: _____
H. J. Staas
Registration No. 22,010

700 Eleventh Street, NW, Suite 500
Washington, D.C. 20001
(202) 434-1500

CERTIFICATE UNDER 37 CFR 1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D.C. 20231

on Monday January 13, 2003

STAAS & HALSEY

By: _____

Date: 1-13-2003

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE ABSTRACT:

Please AMEND the Abstract, as follows:

An authentication apparatus includes a measuring unit [for] measuring biometric information of an individual, a converting unit [for] carrying out a predetermined conversion process with respect to the biometric information so as to obtain converted biometric information, an extracting unit [for] extracting feature information from the converted biometric information so as to obtain extracted feature information, and a verifying unit [for] verifying the extracted feature information with respect to the registered information which is registered in advance, so as to authenticate the individual.

IN THE SPECIFICATION:

Please AMEND the paragraph beginning at page 1, line 7, as follows:

The present invention generally relates to authentication apparatuses and storage mediums, and more particularly to an authentication apparatus which authenticates individuals using biometric information and to a computer-readable storage medium which stores a program for causing a computer to carry out such an authentication.

Please AMEND the paragraph beginning at page 3, line 23, as follows:

Compared to an authentication apparatus which uses a password or the like, the authentication apparatus which uses the biometric information makes it more difficult for a person to assume a false identify. But on the other hand, in the case where the biometric information of the individuals is measured and used in the authentication apparatus, it is necessary to prevent privacy information of the individuals from leaking (i.e., unauthorized disclosure to, or theft thereof by, third parties).

Please AMEND the paragraph spanning pages 3-4, as follows:

Conventionally, stand-alone type authentication apparatuses were the majority, but

recently, the use of client-server type authentication apparatuses coupled to networks has increased. In the case of the client-server type authentication apparatus, it is necessary to register the biometric information of the individuals in a server, and transmit the biometric information via the network. For this reason, if the reliability of the server and/or the network is poor and the data management reliability is not sufficiently high, there [was] is a possibility of the biometric information of the individuals [becoming] being stolen by or [leaking] leaked to an unauthorized third party.

Please AMEND the paragraph beginning at page 11, line 10, as follows:

A description will be given of a first aspect of the present invention. An authentication apparatus shown in FIG. 1A generally includes a measuring means 1 for measuring biometric information of an individual, a converting means 2a for subjecting the biometric information to a predetermined conversion process so as to obtain converted biometric information, an extracting means 3a for extracting feature information from the converted biometric information so as to obtain extracted feature information, and a verifying means 4 for verifying (e.g., by comparing) the extracted feature information with registered information of the individual, which is registered in advance, so as to authenticate the individual.

Please AMEND the paragraph beginning at page 12, line 10, as follows:

Since the registered information is made up of the feature information which is extracted from the biometric information and converted, the original biometric information cannot be read by a third party even if the registered information is stolen or is leaked. As a result, it is possible to positively prevent a leak of privacy information [caused by] even if there is a leak, or a theft, of an individual's extracted and converted biometric information.

Please AMEND the paragraph beginning at page 15, line 7, as follows:

When verifying the biometric information, the converted biometric information verifying unit 15 verifies the verifying biometric information which is obtained from the verifying biometric information generating unit 14, with respect to the registered biometric information which is obtained from the converted biometric information storage managing unit 22, and makes an authentication as to whether or not the user is actually the user himself who is registered. More

particularly, the converted biometric information verifying unit 15 carries out the authentication based on whether or not the [verified] verifying biometric information and the registered biometric information match under a predetermined condition.

IN THE CLAIMS:

Please AMEND the following claims:

17. (ONCE AMENDED) An authentication apparatus for authenticating an individual by verifying input biometric information with respect to registered biometric information, comprising:

measuring means for measuring biometric information of the individual;

converting means for carrying out a predetermined conversion process, selected from a group consisting of expansion, compression, rotation, deformation, affine transformation, morphing, coordinate transformation, function process, parameter conversion, frequency conversion, time base conversion, and rearrangement of bit sequences, with respect to the biometric information so as to obtain converted biometric information; and

registering means for registering the converted biometric information.

25. (ONCE AMENDED) A computer-readable storage medium which stores a program for causing a computer to authenticate an individual by verifying input biometric information with respect to registered biometric information, comprising:

measuring means for causing the computer to measure biometric information of the individual;

converting means for causing the computer to carry out a predetermined conversion process, selected from a group consisting of expansion, compression, rotation, deformation, affine transformation, morphing, coordinate transformation, function process, parameter conversion, frequency conversion, time base conversion, and rearrangement of bit sequences, with respect to the biometric information so as to obtain converted biometric information; and

registering means for causing the computer to register the converted biometric information.

Please ADD the following claims:

27. (NEW) An authentication apparatus, comprising:

a measuring unit measuring biometric information of an individual;

a converter converting the biometric information and outputting converted biometric information;

an extractor extracting feature information from the converted biometric information and outputting extracted feature information; and

a verifier comparing the extracted, converted feature information with registered, corresponding information of the individual, which is registered in advance, to authenticate the individual.

28. (NEW) An authentication apparatus comprising:

a measuring unit measuring biometric information of an individual;

an extractor extracting feature information from the biometric information and outputting extracted feature information;

a converter converting the extracted feature information and outputting converted and extracted feature information; and

a verifier comparing the converted, extracted feature information with registered, corresponding information of the individual, which is registered in advance, to authenticate the individual.

29. (NEW) A computer-readable memory medium which stores a program for causing a computer to authenticate an individual, by:

measuring biometric information of an individual;

converting the measured biometric information to produce converted biometric information;

extracting the converted biometric information to produce extracted, converted feature information; and

comparing the extracted, converted feature information with registered, corresponding information of the individual, which is registered in advance, so as to authenticate the individual.

30. (NEW) A computer-readable memory medium which stores a program for causing a computer to authenticate an individual, by:

measuring biometric information of an individual;

extracting feature information from the measured biometric information and producing extracted feature information;

converting the extracted feature information and producing converted extracted feature information; and

comparing the converted extracted feature information with registered, corresponding information of the individual, which is registered in advance, to authenticate the individual.